

REMARKS

The enclosed is responsive to the Examiner's Office Action mailed on July 24, 2009. At the time the Examiner mailed the Office Action, claims 1, 3-5, 7-17, 19, 21-24 and 27-30 were pending. By way of the present response applicants have: 1) amended no claims; 2) added no claims; and 3) canceled no claims. No new matter has been added. Reconsideration of this application as amended is respectfully requested.

Claim Rejections – 35 U.S.C. §103

Claims 1, 3-5, 7-9, 13, 15-17, 19, 21-24, and 27-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brandys (WO 02/073877A2, hereinafter, "Brandys") in view of Horne (U.S. Patent No. 4,887,296 hereinafter, "Horne") and further in view of Montenegro (U.S. Patent No. 7,434,051 B1 hereinafter, "Montenegro"). Applicants do not admit that Montenegro is prior art and reserve the right to swear behind Montenegro at a later date.

Brandys describes a smart card that verifies biometric information and digitally signs messages upon authenticating a user. In particular, Brandys describes that the smart card signs a message by hashing the message to create a message digest, which is then encrypted with a private key to create a digital signature. A recipient of the message can verify the signature by using a public key.

Horne describes a broadcast satellite system for encrypting audio signals transmitted to a large number of receivers. In particular, Horne describes distributing audio encrypted with a common key. Individual keys for each receiver are generated by encrypting the address number of each receiver using a master

key. The common key is then encrypted using each individual key and transmitted along with the encrypted audio.

Montenegro describes a method for authenticating a Crypto-Based Identifier (CBID) that is transmitted over a public network without a public key infrastructure. In particular, Montenegro describes translating the received CBID is translated using a One-Time Password (OTP) dictionary to display a string of words to the user at the receiving device. The receiving user then verifies the string of words with the sending user - e.g., via a verbal communication.

Applicants submit that Brandys does not teach or suggest a combination with Horne and that Horne does not teach or suggest a combination with Brandys. Brandys describes appending a digital signature to a message - e.g., to a single recipient - based on a private/public key infrastructure and biometric data of the sender so that the sender of the message can be authenticated. In contrast, Horne describes broadcasting encrypted audio in a satellite system to many users - e.g., thousands/millions of recipients. Encryption in Brandys is based upon the sender only, while encryption in Horne is based upon the recipient. The Examiner alleges that the combination would be obvious because "Horne would have improved the teachings of Brandys by using a master key to encrypt generated keys in order to require only a single key to be protected instead of multiple generated keys." (Office Action dated 7/24/09, page 5). Brandys, however, does not disclose protecting or otherwise storing multiple generated keys (e.g., keys for each recipient). Brandys describes storing a single private key/public key pair. Accordingly, applicants submit the combination is the result of impermissible hindsight based solely on applicants'

disclosure and that the Examiner has not articulated a reasoning with some rational underpinning to support the combination of Brandys and Horne.

Furthermore, applicants submit that Horne does not teach or suggest a combination with Montenegro and that Montenegro does not teach or suggest a combination with Horne. Horne describes broadcasting encrypted audio (of satellite TV broadcast) to many recipients - i.e., thousands/millions. Montenegro describes authentication between two users. Furthermore, Montenegro describes translating a CBID into a string that can be read by a user of the receiving device and verified with a user of the sending device so that two users who wish to communicate with each other can authenticate one another's address/devices. Requiring every viewer of a satellite TV broadcast to read a translated string and call the broadcaster to authenticate the CBID each time a connection would render Horne unsatisfactory for its intended purpose. (MPEP § 2143.01V). Accordingly, applicants submit the combination is the result of impermissible hindsight based solely on applicants' disclosure.

Even if Brandys, Horne, and Montenegro were combined, the combination would fail to disclose

wherein the **portable data storage device** is further arranged **to receive** from the host **a digital signature based on the generated key and the requested data transmitted to the host** from the portable storage device, the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host.

(Claim 1) (emphasis added).

Applicants agree with the Examiner that Brandys and Horne fail to disclose this claim feature. Applicants, however, disagree with the allegation that

Montenegro does. Montenegro describes both the recipient and the sender devices using the OTP dictionary to translate a CBID into human-recognizable string of words so that the users of each device can read and compare the strings - e.g., face-to-face, by telephone, etc. Montenegro does not describe that the device that receives the CBID sends a digital signature to the device that sent the CBID.

Additionally, even if the human-recognizable string of words translated from the CBID were considered equivalent to a digital signature (applicants submit that they are not equivalent), the translation is not based upon the generated key and the requested data. Instead, the string is based upon the CBID and the OTP dictionary. The OTP dictionary is not the recited generated key (that was encrypted and transmitted with the requested data).

Furthermore, applicants submit that Montenegro is concerned with authenticating the recipient address and device as belonging to the intended recipient, not verifying that the requested data has been correctly received by the host.

Accordingly, applicants submit that the rejection of claim 1 has been overcome. Given that independent claims 16 and 19, while different from claim 1, contain features similar to claim 1 as discussed above, applicants respectfully submit that the rejection of claims 16 and 19 has been overcome for at least the reasons set forth above.

Given that claims 3-5, 7-9, 13, 15, 17, 21-24 and 27-29 are dependent claims with respect to claims 1, 16, and 19, and include additional features, applicants respectfully submit that the rejection of claims 3-5, 7-9, 13, 15, 17, 21-24 and 27-29 has been overcome for at least the same reasons set forth above.

Claims 10 and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brandys in view of Horne and Montenegro as applied to claims 1 and 19, and further in view of Iwagaki et al., (U.S. Patent Pub No. 2003/0161468 A1 hereinafter, "Iwagaki").

Claims 10 and 30 are dependent upon claims 1 and 19 respectively. Applicants respectfully submit that Iwagaki does not remedy the shortcomings of Brandys, Horne, and Montenegro discussed above. Accordingly, applicants respectfully submit that the rejection of claims 10 and 30 has been overcome for at least the reasons set forth above.

Claims 11, 12, and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brandys in view of Horne and Montenegro as applied to claim 1, and further in view of Fang, (U.S. Patent 6,536,941 hereinafter, "Fang").

Claims 11, 12, and 14 are dependent upon claim 1. Applicants respectfully submit that Fang does not remedy the shortcomings of Brandys, Horne, and Montenegro discussed above. Accordingly, applicants respectfully submit that the rejection of claims 11, 12, and 14 has been overcome for at least the reasons set forth above.

CONCLUSION

Applicants respectfully submit that in view of the amendments and arguments set forth herein, the applicable objections and rejections have been overcome.

Applicants reserve all rights under the doctrine of equivalents.

Pursuant to 37 C.F.R. 1.136(a)(3), applicants hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. 1.16 and 1.17, to Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: October 23, 2009

/Ryan W. Elliott/

Ryan W. Elliott
Reg. No. 60,156

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300